EUTRON
INFOSECURITY

CryptoCombo

Overview version 1.2.2

This hardware key is in compliance with the following test specification:
CEI EN 61000-4-2; CEI EN 61000-4-3; CISPR22
as required by:
CEI EN 61000-6-1, CEI EN 61000-6-2, CEI EN 61000-6-3, CEI EN 61000-6-4
which are specified for the following test:

- “ESD Immunity test”
- “Radiated radio-frequency and electromagnetic field immunity test”
- “Radiated Emission Verification”

In compliance with the “Essential Requisites” for the EMC Directive 89/336/EEC.

FCC ID: TFC-AAD

EUTRON Infosecurity S.r.l.
CryptoCombo [1]
Supply: 5V DC
Absorption: 250 mA

This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) this device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

NOTE: This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.

Caution: changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.

[1] The models subjected to this mark are the following: CryptoCombo ITSEC-I, CryptoCombo ITSEC-P and CryptoCombo FIPS.

IMPORTANT REMARKS

Due to the limited space on the product shell, all FCC certification references are on this technical manual.

Changes or modifications not expressly approved by the party responsible for compliance could void the user’s authority to operate the equipment.

1. Introduction

CRYPTOCOMBO is an “all-in-one” device in a USB key, which offers the following functions:

Smart Card + Smart Card reader + USB memory

Thanks to Smart Card technology, CryptoCombo can securely store in the memory the user’s data (personal profiles, digital certificates, X.509); the flash memory chip on the key allows you to save data and applications, with a self-limiting solution. The private key used to sign electronic documents is securely and secretly stored within a cryptographic chip, thus the access is protected by means of a customizable PIN: having the CryptoCombo hardware device and knowing its PIN are two basic elements of this authentication "double factors" procedure.
CryptoCombo allows you to generate a couple of cryptographic keys within and apply the digital signature. It is equipped with security devices that prevent exporting and copying the private key outside the device that has generated it. The wide memory, both for reading and writing, allows you to transfer data and applications.

When connected to the PC, it will make available as separate resources both an embedded smart card chip (and its reader) and a removable hard drive for general purpose storage.

To put it another way, CryptoCombo is the result of combining, in a single compact USB token, two existing Eutron's products:

- CryptoIdentity, the embedded smart card chip and its reader
- PicoDisk, the removable hard drive for general purpose storage

Therefore,

CRYPTOCOMBO = CryptoIdentity + PicoDisk

and all the documentations, tools, and software do not refer directly to CryptoCombo, but to its constituent parts, CryptoIdentity and PicoDisk. For example, the documentation for CryptoCombo is the combination of the manuals provided for CryptoIdentity and PicoDisk. Similarly, the installation of CryptoCombo results from the installation of CryptoIdentity and PicoDisk.

2. Features

RSA Keys: "on board" generation of the public/private couple of RSA cryptographic keys (up to 2048 bit for CryptoCombo 2048 model). The private key is never exposed to external environment and cannot leave the device. All the public key-based operations are carried out on the token. The public key can be exported at any time.
The multiple memorizations of keys, managed by separated access control mechanisms, are allowed.

User Access: the device is equipped with alphanumeric PIN and PUK, to control the access to data stored in the cryptographic chip memory (usually, digital certificates). In case of several failed access procedures, the user’s PIN is stopped and the token cannot be used any longer.

Standards used: the device supports the following standards: ISO 7816 3-4, USB CCID, PKCS#11 v2.11, PC/SC, Microsoft CAPI, S/MIME, IPSec/IKE and X.509 v3.

Algorithms supported: RSA up to 2048 bit, AES, DES, 3DES, SHA1, MD2, MD5

Cryptographic chip memory: 64 KB

Flash memory: 64MB - 128MB - 256MB - 512MB

Cryptographic chip specifications: chip of the ATMEL AT90SC family with Algorithmic Research mask, able to ensure the secure storage of files and directories within a multilevel hierarchic structure.

Portability: it does not require additional reader, cables or supply batteries. You just have to insert it in the USB port.

Optionals: the device can be supplied with a protective cover for the USB jack. Only for the on-board flash memory, the access is possible without need to install any driver on all Windows operating systems, except for Windows 98 and 98SE.

Small size: 87x17x7 mm

3. System requirements

Hardware requirements:
PC IBM or 100% compatible, Desktop/Notebook/Sub-Notebook/Laptop with USB port (Pentium 100 MHz or higher)

SO requirements:
Microsoft Windows 2000 and Microsoft Windows XP.

Application requirements:
CryptoCombo can interoperate, especially with Netscape Communicator Suite, Microsoft Internet Explorer, Microsoft Outlook, Lotus Notes 6.x, Acrobat 6 or higher and all other applications using supported standards.

4. Technical specifications

- USB Spec. 1.1 - USB 2.0 High Speed
- Green LED (power on/connected)
- Transfer rate of encryption component: up to 64 Kbps
- Data reading speed of the flash memory: 18 MB/s
- Data writing speed on the flash memory: 11 MB/s
- Certifications: FCC/CE

For further information on CryptoCombo visit:
www.cryptocombo.eutron.com